JENNIFER M. GRANHOLM
GOVERNOR

STATE OF MICHIGAN
OFFICE OF FINANCIAL AND INSURANCE SERVICES
DEPARTMENT OF LABOR & ECONOMIC GROWTH
DAVID C. HOLLISTER, DIRECTOR

LINDA A. WATTERS
COMMISSIONER

DATE: February 3, 2004

LETTER NO.: 2004-CU-01

TO: The Board of Directors and Management of Michigan State-Chartered Credit Unions

SUBJECT: Information Technology Examinations

Summary
Recognizing the significance of Information Technology (IT) and the rapid advancements in core processing and in delivery channels of customer products and services, the Office of Financial and Insurance Services (OFIS) is instituting changes to the IT examination process effective February 1, 2004. The most notable changes include the disclosure of IT component and composite ratings and a redesigned Website Review Report. These changes, discussed in detail below, are designed to facilitate communication of IT related strengths and weaknesses, prioritize regulatory concerns, create an open dialogue on rating factors, and improve the quality of information provided to credit union management in monitoring IT risk.

IT Examination Rating Disclosure
OFIS IT examinations will assign ratings based on guidelines established by the Federal Financial Institutions Examination Council (FFIEC). The component ratings include: Audit, Management, Systems Development and Programming, and Operations. These four component sections will be compiled into one composite rating. Each component section will be evaluated on a scale of '1' to '5', with '1' rated 'strong performance' and '5' rated 'hazardous performance'. Results of the IT component rating will be a factor in the evaluation of the 'Management Effectiveness' component of the CAMEL rating system. All regulatory examination reports are provided for the sole use of credit union executive management and directors. As such, disclosure of any rating is prohibited unless express permission is granted, in writing, by this office.

The IT component sections of Audit, Management, Systems Development and Programming and Operations encompass the following areas:

Audit	Management
▶Audit Overview ▶Audit Organization ▶Audit Staffing ▶Internal/External Activities	▶Effectiveness ▶Correction of Deficiencies ▶Compliance Performance ▶Planning and Direction ▶Corporate Information Security Program ▶Corporate Contingency Planning ▶Standards and Procedures ▶Internal Controls ▶Physical Security ▶Adequacy of MIS (if applicable) ▶Financial Condition

Systems Development and Programming	Operations
▶S&P Organization ▶Staffing ▶Standards and Procedures ▶Documentation ▶Internal Controls ▶Physical Security	▶Operations Organization ▶Staffing ▶Standards and Procedures ▶Operations/Processing Concerns ▶Operations Activities

Historically, the IT Examinations Group internally rated credit unions on the above criteria but did not disclose ratings to management. IT ratings are focused on people, policy, procedures, and programming risks. Examiners will use subjective judgment when issuing the IT component ratings. IT exams will continue to evolve, focusing on emerging risk areas and risk measurement tools.

OFIS believes IT ratings disclosure will facilitate communication and greater understanding of identified risks between this office and the institution. Reporting to management, including the Directorate, will include IT risk measurements in a standardized format which will identify the nature and perceived significance of problem areas.

Redesigned Website Review Report

The redesigned Website Review Report prioritizes regulatory concerns, while reporting inherent risk and management's adequacy of mitigating practices related to the credit unions' websites. The redesigned report categorizes regulatory concerns and violations into three major risk areas: legal, reputational, and operational. The report also prioritizes risk areas/violations from high to low.

The new format uses a website risk matrix. The matrix interlays three types of risks (legal, reputational, and operational) with a ranking of the degree of inherent risk and the assessment of risk management. These two rankings are combined to arrive at a Composite Risk Rating. Inherent risk and the Composite Risk Rating are rated as low, moderate, or high. Risk management is rated as weak, acceptable, or strong.

The following describes the inherent risk categories:

> *High Risk* - The activity potentially could result in a significant and harmful loss to the organization.
> *Moderate Risk* - The activity potentially could result in a loss to the organization, and the loss could be absorbed by the organization in the normal course of business.
> *Low* Risk - The risk of loss is remote or, if a loss were to occur, it would have little negative impact on the institution's overall financial condition.

The following paragraph describes the risk management assessment definitions:

> *Strong* - Management effectively identifies and controls the risk in question. The board and management participate in managing risk and ensuring appropriate policies and limits exist. These policies and limits provide the necessary information and analyses to make timely and appropriate decisions to the activities of the institution. There are few exceptions to established polices and procedures, and none of these exceptions would likely lead to a significant loss to the institution.
> *Acceptable* - The institution's risk management systems, although largely effective, may be lacking. Systems are able to cope with existing and foreseeable exposure arising in carrying out the institution's business plan. While the institution may have some minor risk management weaknesses, these problems have been recognized and are being addressed. Overall, board and senior management oversight, policies and limits, risk-monitoring procedures, reports and MIS are considered effective in maintaining a safe and sound institution. Risks are generally controlled in a manner that does not require more than normal supervisory attention.
> *Weak* - Systems are lacking in important ways and require additional supervisory attention. The internal control system may be lacking in important respects, particularly as indicated by continued control exceptions or by the failure to adhere to written policies and procedures. The deficiencies associated with these systems could have adverse affects on the safety and soundness of the institution. The deficiencies lead to material negative impact of an institution's financial statements.

An example website risk matrix table is shown below:

Type of Risk	Inherent Risk	Risk Management	Composite Risk Rating
Legal Reputational Operational	Moderate	Strong	Low

- Inherent Risk is defined as the amount of risk implicitly associated within a certain program.
- Risk Management is defined as management's approach in managing risks within a certain program.
- Composite Risk Rating is defined as how well is management actively managing inherent risk within a certain program.

In the above example, the credit union's website program contains 'moderate' inherent exposure to legal risk. Management's development of a superior internal control environment results in a 'strong' Risk Management rating. As a result, the Composite Risk Rating is 'low', given managements proactive oversight of the program risk.

Conclusion

OFIS continues to strive as a proactive regulator that uses open dialogue with credit unions. The IT changes were designed to improve the communication process on high emerging risk areas. These changes should facilitate the communication of risks and expectations clearly to management.

If you have any questions or comments concerning these changes, please call Brent Moeggenborg, IT Manager, (517-373-6930).

Sincerely,

Roger W. Little, Deputy Commissioner
Credit Union Division